Attorney Docket No. RSW920010222US1 (5577-351) PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson et al.
Serial No.: 10/007,582
Filed: December 5, 2001
For: OFFLOAD PROCESSING FOR SECURE DATA TRANSFER

Confirmation No.: 3561
Examiner: Joseph T. Pan
Group Art Unit: 2135

Date: June 4, 2007

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION
I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on June 4, 2007

Signature: Amelia Tauchen
Amelia Tauchen

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith is the APPEAL BRIEF for the above-identified application, pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed April 4, 2007 and the "Notice of Panel Decision from Pre-Appeal Brief Review" mailed April 30, 2007.

2. This application is filed on behalf of
☐ a small entity.

3. Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

☐	small entity	$250.00
☒	other than small entity	$500.00

Appeal Brief fee due $500.00

☒ Please charge IBM's Deposit Account No. 09-0461 in the amount $500. Any additional fee or refund may be charged to IBM's Deposit Account No. 09-0461.

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 46589

Respectfully submitted,

D. Scott Moore
Registration No.: 42,011

Attorney Docket No. RSW920010222US1 (5577-351) PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson et al.
Serial No.: 10/007,582
Filed: December 5, 2001
For: OFFLOAD PROCESSING FOR SECURE DATA TRANSFER

Confirmation No.: 3561
Examiner: Joseph T. Pan
Group Art Unit: 2135

Date: June 4, 2007

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION
I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on June 4, 2007

Signature: Amelia Tauchen
Amelia Tauchen

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed April 4, 2007 and the "Notice of Panel Decision from Pre-Appeal Brief Review" mailed April 30, 2007.

Real Party In Interest

The real party in interest is assignee International Business Machines, Inc., Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present appeal.

Status of Claims

Appellants appeal the final rejection of Claims 1 - 20 as set forth in the Final Office Action of January 4, 2007 (hereinafter "Final Action"). Claims 1 – 20 stand rejected. Appellants submit that the claims involved in the appeal are Claims 1 - 20 as a reversal of the rejection of independent Claims 1, 12, and 13 is requested in the present appeal and a reversal of the rejection of dependent Claims 2 – 11, and 14 - 20 is also requested based, at least, on the reversal of the rejection of independent Claims 1, 12, and 13. The claims involved in the appeal as included in Appellants response to the Office Action of June 21, 2006 are attached hereto as Appendix A.

Status of Amendments

No amendment has been filed in the present case in response to the Final Action.

Summary of Claimed Subject Matter

Independent Claim 1 is directed to a method of improving security processing in a computing network. The method includes the following: providing a security offload component in an operating system kernel, which performs security processing (Specification, page 11, lines 13 – 19); providing control functions in the operating system kernel for directing operation of the security offload component (system SSL calls in TCP layer in FIGS. 2A – 2E; Specification, page 12, line 9 – page 18, line 14); providing an application program (application layer in FIGS. 2A- 2E; Specification, page 12, line 9 – page 18, line 14); executing the application program (description of application layer of FIGS. 2A – 2E; Specification, page 12, line 9 - page 18, line 14); and executing the provided control functions during execution of the application program, thereby selectably directing the security offload component to secure at least one communication of the executing application program (description of security processing scenarios with respect to FIGS. 2A – 2E; Specification, page 12, line 9 – page 18, line 14).

Independent Claim 12 is directed to a system for improving security processing in a computing network. The system includes the following: a security offload component in an operating system kernel which performs security processing (Specification, page 11, lines 13 – 19); at least one control function in the operating system kernel for directing operation of the

security offload component (system SSL calls in TCP layer in FIGS. 2A – 2E; Specification, page 12, line 9 – page 18, line 14); means for executing the at least one provided control function (client system/server system and associated logic; FIGS. 3 – 8; Specification, page 22, line 4 – page 33, line 11); and means, responsive to operation of the means for executing, for directing the security offload component to secure at least one communication of an application program (client system/server system and associated logic; FIGS. 3 – 8; Specification, page 22, line 4 – page 33, line 11). The client/server systems and associated logic represented by FIGS. 3 – 8 provide the structure for the means for executing and the means for directing.

Independent Claim 13 is directed to a computer program product for improving security processing in a computing network. The computer program product is embodied on at least one computer-readable medium and includes the following: a security offload component in an operating system kernel which performs security processing (Specification, page 11, lines 13 – 19); at least one control function in the operating system kernel for directing operation of the security offload component (system SSL calls in TCP layer in FIGS. 2A – 2E; Specification, page 12, line 9 – page 18, line 14); computer-readable program code for executing the at least one provided control function (client system/server system and associated logic; FIGS. 3 – 8; Specification, page 22, line 4 – page 33, line 11); and computer-readable program code, responsive to operation of the computer-readable program code for executing, for directing the security offload component to secure at least one communication of an application program (client system/server system and associated logic; FIGS. 3 – 8; Specification, page 22, line 4 – page 33, line 11).

Grounds of Rejection to be Reviewed on Appeal

Independent Claims 1, 12, and 13 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 6,370,599 to Anand et al. (hereinafter "Anand").

Argument

I. Introduction to 35 U.S.C. §102 Analysis

Under 35 U.S.C. § 102, "a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (quoting *Verdegaal Bros. v. Union Oil Co.*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)). "Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." *Apple Computer Inc. v. Articulate Sys. Inc.*, 57 U.S.P.Q.2d 1057, 1061 (Fed. Cir. 2000). "The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" M.P.E.P. § 2112 (citations omitted).

A finding of anticipation further requires that there must be no difference between the claimed invention and the disclosure of the cited reference as viewed by one of ordinary skill in the art. *See Scripps Clinic & Research Foundation v. Genentech Inc.*, 927 F.2d 1565, 1576, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991). In particular, the Court of Appeals for the Federal Circuit held that a finding of anticipation requires absolute identity for each and every element set forth in the claimed invention. *See Trintec Indus. Inc. v. Top-U.S.A. Corp.*, 63 U.S.P.Q.2d 1597 (Fed. Cir. 2002). Additionally, the cited prior art reference must be enabling, thereby placing the allegedly disclosed matter in the possession of the public. *In re Brown*, 329 F.2d 1006, 1011, 141 U.S.P.Q. 245, 249 (C.C.P.A. 1964). Thus, the prior art reference must adequately describe the claimed invention so that a person of ordinary skill in the art could make and use the invention.

Appellants respectfully submit that the pending claims are patentable over the cited reference for at least the reason that the cited reference does not disclose or suggest each of the recitations of the independent claims. The patentability of the pending claims is discussed in detail hereinafter.

A. Independent Claims 1, 12 and 13 are Patentable over Anand

Independent Claims 1, 12, and 13 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 6,370,599 to Anand. (Final Action, page 2). Independent Claims 1, 12, and 13 are directed to a method, a system, and a computer program product for improving security processing in a computing network in which a security offload component is used. In particular, these three claims describe the security offload component as being in the operating system kernel. For example, independent Claim 1 recites:

> **providing a security offload component in an operating system kernel** which performs security processing;
> providing control functions in the operating system kernel for directing operation of the security offload component;
> providing an application program;
> executing the application program; and
> executing the provided control functions during execution of the application program, thereby selectably directing the security offload component to secure at least one communication of the executing application program. (Emphasis added.)

Claims 12 and 13 include similar recitations. Support for providing the security offload component as part of the operating system kernel is provided, for example, at page 11, lines 13 - 19 of the Specification. Specifically, the Specification states:

> The present invention moves security processing (or control thereof) for security protocols such as SSL and TLS (which are connection-oriented protocols) into the kernel. In several embodiments, the security processing is performed in the TCP layer. (Specification, page 11, lines 13 - 15; emphasis added).

The Final Action cites FIG. 2 and various passages from the Abstract and Summary sections of Anand as disclosing the recitations of independent Claims 1, 12, and 13. (Final Action, pages 2 - 5). Appellants respectfully submit, however, that the Final Action appears to have misinterpreted the teachings of Anand. As highlighted above, independent Claims 1, 12, and 13 include recitations directed to providing a security offload component in an operating system kernel. That is, the security offload component is provided as part of the operating

system kernel software. In sharp contrast, Anand is directed to moving tasks that are typically performed in software to a hardware component. (Anand, col. 1, lines 20 - 27). Anand explains this goal of moving tasks from software to hardware in more detail as follows:

> Embodiments of the present invention are directed to providing the ability to reducing the processing overhead and memory usage of a processing unit 21. This is accomplished by offloading particular computing tasks, which are accomplished for instance by way of an operating system, application programs and/or other program modules that are executing on the processing unit/CPU 21, to an appropriate peripheral hardware device connected to the computer system 20. (Anand, col. 7, lines 47 - 55; emphasis added).

Rather than move a security offload component into the kernel of the operating system as recited in Claims 1, 12, and 13, Anand specifically contemplates moving tasks performed by operating system software to a peripheral hardware device in the passage reproduced above. With respect to the specific function of IP security (see, IP Security function 144 of FIG. 3 of Anand), Anand does not suggest moving such functionality into the operating system kernel, but instead suggests moving such functionality into the network interface card (NIC) 100 hardware. (*See, e.g.*, Anand, col. 11, lines 2 - 6 and col. 12, lines 15 - 19).

In response to this argument, the Final Action appears to state that the Specification does not support a recitation directed to a security offload component that is in an operating system kernel. (Final Action, pages 6 and 7). Appellants respectfully disagree. As reproduced above, the first sentence of the "Description Of Preferred Embodiments" provides support for security processing being moved into the operating system kernel such as, for example, into the TCP layer. Appellants submit that it is common usage to call a piece of software a "component" or "module." Thus, Claim 1 recites this aspect of the present invention as "**providing a security offload component in an operating system kernel** which performs security processing." The Final Action proceeds to quote several passages from the Specification that describe a "security offload component" or "encryption component" as being a hardware device. (Final Action, pages 7 - 9). Appellants agree that the Specification describes several embodiments in which a security offload component is implemented as a hardware device. But as highlighted above, the Specification also describes numerous embodiments in which security processing is offloaded

from the application into the operating system kernel, such as the TCP layer, as discussed with reference to FIGS. 2A through 2E.

Appellants further submit that Anand inherently does not disclose or suggest the recitation "providing control functions in the operating system kernel for directing operation of the security offload component" of Claim 1 and analogous recitations of Claims 12 and 13 as Anand describes moving the security functionality into a hardware component, such as a NIC, to relieve the CPU, which executes the operating system software, of that task. (*See, e.g.*, above discussion and Anand, col. 3, lines 18 - 22).

For at least the foregoing reasons, Appellants respectfully submit that independent Claims 1, 12 and 13 are patentable over Anand and that dependent Claims 2 – 11 and 14 - 20 are patentable at least by virtue of their depending from an allowable claim. Accordingly, Appellants respectfully request that the rejection of independent Claims 1, 12, and 13 be reversed based on the failure of the Examiner to establish a prima facie case of anticipation under 35 U.S.C. §102 for at least these reasons.

B. Dependent Claims 8 – 11 and 17 are Patentable over Anand

As discussed above, dependent Claims 8 – 11 and 17 are patentable as least as they depend from a patentable independent claim. Appellants further submit, however, that these dependent claims are separately patentable for at least the reasons discussed hereafter.

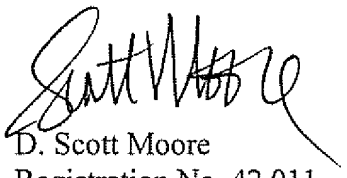
Dependent Claims 8 – 11 and 17 stand rejected under 35 U.S.C. §102(e) as being anticipated by Anand. Each of dependent Claims 8 - 10 provides additional details with respect to what is provided to the security offload component for use in securing communications. Dependent Claims 11 and 17 provide additional detail with respect to how outbound data is sent from the security offload component. As discussed above, Anand does not disclose or suggest providing a security offload component as part of the operating system kernel. While Appellants acknowledge that Anand does suggest that certain security functionality may be provided by a hardware peripheral (see, e.g., Anand, col. 2, lines 55 - 60), Appellants submit that Anand does not appear to disclose any of the specific details of dependent Claims 8 - 10, 11, and 17. Accordingly, for at least the foregoing reasons, Appellants respectfully submit that dependent Claims 8 - 11 and 17 are separately patentable over Anand. Appellants respectfully request that

the rejection of dependent Claims 8 – 11 and 17 be reversed based on the failure of the Examiner to establish a prima facie case of anticipation under 35 U.S.C. §102 for at least these additional reasons.

II. Conclusion

In summary, Appellants respectfully submit that, with respect to Claims 1 - 20, the cited reference does not teach all of the recitations of the claims. Accordingly, Appellants respectfully request reversal of the rejection of Claims 1 - 20 based on the cited reference.

Respectfully submitted,



D. Scott Moore
Registration No. 42,011

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 46589

APPENDIX A – CLAIMS APPENDIX

1. (Previously presented) A method of improving security processing in a computing network, comprising:

providing a security offload component in an operating system kernel which performs security processing;

providing control functions in the operating system kernel for directing operation of the security offload component;

providing an application program;

executing the application program; and

executing the provided control functions during execution of the application program, thereby selectably directing the security offload component to secure at least one communication of the executing application program.

2. (Previously presented) The method according to Claim 1, wherein the executing control functions comprises a function directing the security offload component to begin securing the communications.

3. (Previously presented) The method according to Claim 1, wherein the executing control functions comprises a function directing the security offload component to stop securing the communications.

4. (Original) The method according to Claim 2, wherein the function further specifies information to be used by the security offload component.

5. (Previously presented) The method according to Claim 4, wherein the specified information comprises at least one of: authentication information; cipher suites options; and security key input information.

6. (Original) The method according to Claim 1, wherein the control functions further inform protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

7. (Previously presented) The method according to Claim 6, wherein the modifications comprise reserving space in the outbound data for security headers and trailers.

8. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing at least one of client and/or server certificates to the security offload component for use in securing the communications.

9. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing at least one key or key ring to the security offload component for use in securing the communications.

10. (Previously presented) The method according to Claim 1, wherein the control functions comprise providing an identification of a encryption algorithm to the security offload component for use in securing the communications.

11. (Original) The method according to Claim 1, wherein secured outbound data of the executing application is thereby sent to its destination directly from the security offload component, after a single pass over a data bus from a protocol stack of the operating system kernel.

12. (Previously presented) A system for improving security processing in a computing network, comprising:

a security offload component in an operating system kernel which performs security processing;

at least one control function in the operating system kernel for directing operation of the security offload component;

means for executing the at least one provided control function; and

means, responsive to operation of the means for executing, for directing the security offload component to secure at least one communication of an application program.

13. (Previously presented) A computer program product for improving security processing in a computing network, the computer program product embodied on at least one computer-readable media and comprising:

a security offload component in an operating system kernel which performs security processing;

at least one control function in the operating system kernel for directing operation of the security offload component;

computer-readable program code for executing the at least one provided control function; and

computer-readable program code, responsive to operation of the computer-readable program code for executing, for directing the security offload component to secure at least one communication of an application program.

14. (Previously presented) The system according to Claim 12, wherein the means for executing comprises means for directing the security offload component to begin securing the communications.

15. (Previously presented) The system according to Claim 12, wherein the means for executing comprises means for directing the security offload component to stop securing the communications.

16. (Previously presented) The system according to Claim 12, wherein the at least one control function further informs protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

17. (Previously presented) The system according to Claim 12, wherein secured outbound data of the application program is thereby sent to its destination directly from the security offload component, after a single pass over a data bus from a protocol stack of the operating system kernel.

18. (Previously presented) The computer program product according to Claim 13, wherein the computer readable program code for executing comprises computer readable program code for directing the security offload component to begin securing the communications.

19. (Previously presented) The computer program product according to Claim 13, wherein the computer readable program code for executing comprises computer readable program code for directing the security offload component to stop securing the communications.

20. (Previously presented) The computer program product according to Claim 13, wherein the at least one control function further informs protocol layers of the operating system kernel to modify outbound data in preparation for use by the security offload component.

APPENDIX B – EVIDENCE APPENDIX

None

APPENDIX C – RELATED PROCEEDINGS APPENDIX

None.